BANK PHISHING SMSen

Smishing (eng Kombinatioun aus de Wierder SMS a Phishing) ass e Versuch vun de Schwindler, perséinlech, Finanz oder Sécherheets-Informatiounen iwwer SMSen ze kréien.

WÉI FONCTIONNÉIERT DAT?

An der SMS gitt Dir gewéinlech gebieden, op a Link ze klicken oder eng Telefonsnummer unzeruffen fir äre Kont ze “iwwerpréiwen”, z’”aktualiséieren” oder ze “reaktivéieren”. Mee de Link féiert zu enger falscher Websäit an d’Telefonsnummer gehéiert dem Schwindler, deen ugëtt eng legitim Gesellschaft ze sinn.

WAT KËNNT DIR MAACHEN?

- **Klickt net op Linken, Unhäng oder Biller**, déi Dir an ongefrote SMSen kritt ouni fir d’éischt den Absender ze kontrolléieren.
- **Sidd net presséiert**. Huelt Iech Zäit fir déi néideg Iwwerpréiwungen ze maachen, ier Dir äntwert.
- **Äntwert ni op eng SMS**, déi Iech äre PIN, ärt OnlineBanking-Passwuert oder och är Sécherheetsdonnéeë freet.
- Wann Dir méngt, datt Dir op eng Smishing-SMS geäntwert hutt an är Bankdonnéeë erausginn hutt, **kontaktéiert direkt är Bank**.

#CyberScams

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | THE GOVERNMENT OF THE GRAND DUCHY OF LUXEMBOURG Ministry of the Economy | ABBL | SECURITY MADEIN.LU | BEE SECURE